

REMARKS

Applicants respectfully request further examination and reconsideration in view of the instant response. Claims 1-20 remain pending in the case. Claims 1-20 are rejected.

35 U.S.C. §103(a)

Claims 1-3, 6-10 and 14-20 stand rejected under 35 U.S.C. §103(a) as being unpatentable over United States Patent 6,028,932 by Park, hereinafter referred to as the "Park" reference, in view of United States Patent 6,058,476 by Matsuzaki, hereinafter referred to as the "Matsuzaki" reference. Applicants have reviewed the cited references and respectfully submit that the embodiments of the present invention as recited in Claims 1-3, 6-10 and 14-20 are not unpatentable over Park in view of Matsuzaki.

Applicants respectfully direct the Examiner to independent Claim 1 that recites that an embodiment of the present invention is directed to (emphasis added):

A system for transferring information, said system comprising:

a source device for encoding an encryption mode identifier (EMI) code into an information packet and for transmitting said information packet over a communication interface, said source device comprising:

a first encryption circuit for encrypting data of said information packet provided said EMI code indicates a first mode; and

a second encryption circuit for encrypting said data of said information packet provided said EMI code indicates a second mode; and
a sink device for receiving said information packet from said communication interface, said sink device comprising:
an extractor circuit for extracting said EMI code from said information packet; and
a second decryption circuit for decrypting said data of said information packet in response to said extractor circuit indicating that said EMI code is of said second mode; and
wherein said first mode is a copy prohibition mode indicating that said information packet is not to be reproduced by said sink device and wherein said second mode is a copy once inhibition mode indicating that said information packet is not to be reproduced more than once by said sink device.

Independent Claims 8 and 15 recite similar limitations. Claims 2, 3 and 6 that depend from independent Claim 1, Claims 9, 10 and 14 that depend from independent Claim 8, and Claims 16-20 that depend on independent Claim 15 provide further recitations of features of the present invention.

The claimed embodiments of the present invention are related to an information system that utilizes an EMI code transmitted between a source and a sink for performing two function: 1) selecting between different encryption modes for encrypting information packets transmitted from the source device to the sink device and the also 2) indicates a level of copy protection allowed for the packet. Depending on which secure mode is selected, a different encryption process is used by the source device to encrypt the transmission. Further, depending on which secure mode is selected, a different decryption process is used by the sink device to decrypt the transmission.

Applicants respectfully assert that Claims 1, 8 and 15 overcome the combination of Park and Matsuzaki because the combination of Park and Matsuzaki does not teach or suggest these claimed features. Park and the claimed invention are very different. For instance, Applicants understand Park to teach a copy prevention apparatus for a digital video system. In particular, Park teaches a device for reproducing data that includes a single decryption means for decrypting the output and transmitting it to a recording-side VCR. As acknowledged by the Examiner, Park does not teach a source device including a first decryption unit and a second decryption unit or a common encryption unit for providing different encryption modes, as claimed.

With reference to Figure 5 of Park, a copy prevention apparatus is shown including a reproducing portion 1 for reproducing data recorded on tape, a key inserting portion 2 for adding a tape header start code and key field at the front end of a bit stream of reproducing portion 1, and a decrypting portion 3 for decrypting the output of key inserting portion 2 and transmitting it as parallel data to a recording-side VCR (col. 3, lines 58-65). Specifically, Park teaches the use of public key encryption where data is decrypted according to a key, and the decrypted data and the key are both transmitted to a recording device. In order to record the decrypted data at the recording-side VCR, the reproducing-side VCR must transmit its unique key to the recording-side VCR, thus allowing the recording-side VCR to encrypt the data according to the unique key (col. 5, lines 21-31).

Moreover, as shown in Figure 5, Park teaches a copy prevention apparatus including a key detecting/correcting portion 4 for detecting a key field from the parallel data transmitted from decrypting portion 3 and an encrypting portion 7 for encrypting the output of copy in order to make a recording of the copy. As described above, encrypting the data requires the receipt of a key as detected by key detecting/correcting portion 4. Applicants respectfully assert that Park teaches a reproducing-side device for decrypting data and transmitting it to a recording-side device along with a key, wherein the recording-side device is for encrypting the data based on the key. In contrast, by teaching the transmission of decrypted data along with a key, Park teaches away from the present invention as claimed.

Moreover, the combination of Park and Matsuzaki fails to teach or suggest the claimed invention, because Matsuzaki does not overcome the shortcomings of Park. Matsuzaki, alone or in combination with Park, does not show or suggest the claim embodiments. As described above, Park teaches a device for reproducing data that includes a single decryption means for decrypting the output and transmitting it to a recording-side VCR.

Applicants understand Matsuzaki to teach an encryption apparatus for ensuring security communication between devices. In particular, Matsuzaki teaches a first device and a second device that are each equipped with an

encryption algorithm. With reference to Figure 3 of Matsuzaki, the transmission of copyrighted material mj from first device 51 to second device 52 is shown. Specifically, first device 51 includes first encryption IC 54 and second device 52 includes second encryption IC 56 (col. 11, lines 12-32). First encryption IC 54 and second encryption IC 56, located respectively in separate devices, transmit and receive data between each other and other components of the devices to facilitate the transfer of the copyrighted material. Each of first encryption IC 54 and second encryption IC 56 perform different steps in the processing sequence for transferring data, and are thus both utilized in a single encryption/decryption scheme (col. 11, lines 26-29 and 39-42). In particular, first encryption IC 54 employs an encryption algorithm and second encryption IC 56 employs the complementary decryption algorithm (col. 11, lines 43-61). By teaching that each device includes a single encryption IC, Matsuzaki teaches away from a source device including a first decryption unit and a second decryption unit or a common encryption unit for providing different encryption modes, as claimed.

Therefore, Applicants respectfully assert that nowhere does the combination of Park in view of Matsuzaki teach, disclose or suggest the claimed embodiments of the present invention as recited in independent Claims 1, 8 and 15, and that these claims are thus in a condition for allowance. Applicants respectfully submit that the combination of Park in view of Matsuzaki also does not teach or suggest the additional claimed features of the present

invention as recited in Claims 2, 3 and 6 that depend from independent Claim 1, Claims 9, 10 and 14 that depend from independent Claim 8, and Claims 16-20 that depend on independent Claim 15. Therefore, Applicants respectfully submit that Claims 2, 3, 6, 9, 10 and 16-20 overcome the rejection under 35 U.S.C. § 103(a), and are in a condition for allowance as being dependent on an allowable base claim.

Claims 1, 3-8, 10-13, 15, 16 and 18 stand rejected under 35 U.S.C. §103(a) as being unpatentable over United States Patent 6,047,103 by Yamauchi et al., hereinafter referred to as the "Yamauchi" reference, in view of Matsuzaki. Applicants have reviewed the cited references and respectfully submit that the embodiments of the present invention as recited in Claims 1, 3-8, 10-13, 15, 16 and 18 are not unpatentable over Yamauchi in view of Matsuzaki.

As described above, independent Claims 1, 8 and 15 of the present invention are directed towards an information system that utilizes an EMI code transmitted between a source device and a sink device for encrypting information packets transmitted from the source device to the sink device at a selected level of copy protection. As claimed, the source device includes a first encryption circuit and a second encryption circuit. In particular, the first encryption circuit and a second encryption circuit operate independently to encrypt data using different modes. With reference to Figure 5A of the present

specification, broadcast receiver device 120 includes encrypt unit A 418 and encrypt unit B 420. As described in the accompanying specification, encrypt unit A 418 and encrypt unit B 420 provide different EMI encryption modes (page 15, line 19 through page 16, line 12).

Applicants respectfully assert that Claims 1, 8 and 15 overcome the combination of Yamauchi and Matsuzaki because the combination of Yamauchi and Matsuzaki does not teach or suggest these claimed features. For instance, Yamauchi and the claimed invention are very different. Applicants understand Yamauchi to teach a data transmitting device capable of performing copyright protection processing. In particular, Yamauchi teaches an information processing apparatus including a disk reproduction drive having a single encrypting section. As acknowledged by the Examiner, Yamauchi does not teach, describe or suggest that the encrypting section provides two different encryption modes. Moreover, Applicants respectfully assert that by teaching a single encryption section while remaining silent as to its operation, Yamauchi teaches away from such a configuration.

Moreover, independent Claims 1 and 8 are directed towards an information system that includes a sink device including an extractor circuit. With reference to Figure 5A of the present specification, sink device 130 includes EMI extractor 440 (page 16, lines 18-25). In particular, the extractor circuit is comprised within the sink device.

In contrast, Applicants understand Yamauchi to teach an information processing apparatus including a disk reproduction drive, an AV signal processor, and a controller, wherein each component is discrete and coupled to an I/O bus. With reference to Figure 15 of Yamauchi, an information processing apparatus is shown including disk reproduction drive 125, AV signal processor 126, and controller 128. In particular, controller 128 is not comprised within AV signal processor 126. On the contrary, by teaching that AV signal processor 126 does not include controller 128, Yamauchi teaches away from such a configuration.

Furthermore, the combination of Yamauchi and Matsuzaki fails to teach or suggest the claimed invention, because Matsuzaki does not overcome the shortcomings of Yamauchi. Matsuzaki, alone or in combination with Yamauchi, does not show or suggest the claim embodiments. As described above, Yamauchi teaches a single encryption section operable to provide a single encryption mode.

As described above, Applicants understand Matsuzaki to teach an encryption apparatus for ensuring security communication between devices. In particular, Matsuzaki teaches a first device and a second device that are each equipped with an encryption algorithm. In particular, the first encryption of the first device employs an encryption algorithm and a second encryption IC of the

second device employs the complementary decryption algorithm (col. 11, lines 43-61). By teaching that each device includes a single encryption IC, Matsuzaki teaches away from a source device including a first decryption unit and a second decryption unit or a common encryption unit for providing different encryption modes, as claimed.

Therefore, Applicants respectfully assert that nowhere does the combination of Yamauchi in view of Matsuzaki teach, disclose or suggest the claimed embodiments of the present invention as recited in independent Claims 1, 8 and 15, and that these claims are thus in a condition for allowance. Applicants respectfully submit that the combination of Yamauchi in view of Matsuzaki also does not teach or suggest the additional claimed features of the present invention as recited in Claims 3-7 that depend from independent Claim 1, Claims 10-13 that depend from independent Claim 8, and Claims 16 and 18 that depend on independent Claim 15. Therefore, Applicants respectfully submit that Claims 3-7, 10-13, 16 and 18 overcome the rejection under 35 U.S.C. § 103(a), and are in a condition for allowance as being dependent on an allowable base claim.

CONCLUSION

Based on the arguments presented above, Applicants respectfully assert that Claims 1-20 overcome the rejections of record and, therefore, Applicants respectfully solicit allowance of these Claims.

The Examiner is invited to contact Applicants' undersigned representative if the Examiner believes such action would expedite resolution of the present Application.

Respectfully submitted,

WAGNER, MURABITO & HAO L.L.P.

Dated: 17 Aug, 2005



Matthew J. Blecher
Registration No. 46,558

Two North Market Street
Third Floor
San Jose, CA 95113
(408) 938-9060